AO 91 (Rev. 11/82)

CRIMINAL COMPLAINT

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v. JOADLY SERRANO and JOSE LUIS MIRANDA	DOCKET NO. MAGISTRATE'S CASE NO. 18MJ02768

Complaint for violation of Title 18, United States Code, Sections 1708 and 2

NAME OF MAGISTRATE JUDGE		LOCATION
THE HONORABLE SUZANNE H. SEGAL	UNITED STATES MAGISTRATE JUDGE	Los Angeles, California

DATE OF OFFENSE	PLACE OF OFFENSE	ADDRESS OF ACCUSED (IF KNOWN)
October 2, 2018	Los Angeles County	

CLERK U.S. DISTRICT COURT
OCT 18 2018
CENTRAL DISTRICT OF CALIFORNIA
BY

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

[18 U.S.C. §§ 1708 and 2]

On or about October 2, 2018, in Los Angeles County, within the Central District of California, defendants JOADLY SERRANO and JOSE LUIS MIRANDA did steal and take from and out of an authorized depository for mail matter located at El Dorado Lofts, 416 South Spring Street, Los Angeles, California, in violation of Title 18, United States Code, Sections 1708 and 2.

FILED
2018 OCT 18 PM 1:
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES

BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:

(See attached affidavit which is incorporated as part of this Complaint)

MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.

SIGNATURE OF COMPLAINANT: /s/ James Keenan

OFFICIAL TITLE: U.S. Postal Inspector, U.S. Postal Inspection Service

Sworn to before me and subscribed in my presence,

SIGNATURE OF MAGISTRATE JUDGE[1]: Suzanne H. Segal — SUZANNE H. SEGAL

DATE: October 18, 2018

[1] See Federal Rules of Criminal Procedure 3 and 54

AUSA Catherine S. Ahn x2424 REC: Detention

AFFIDAVIT

I, James Keenan, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against and an arrest warrant for JOADLY SERRANO ("SERRANO"), JOSE LUIS MIRANDA ("MIRANDA"), and YESENIA TORRES ("TORRES"), for mail theft and aiding and abetting mail theft, in violation of 18 U.S.C. §§ 1708 and 2.

2. This affidavit is also made in support of an application to search the person of SERRANO, as described more fully in Attachment A-1, the person of TORRES, as described more fully in Attachment A-2, a red 2017 Toyota with California license plate tag 7ZOT239 (the "SUBJECT VEHICLE"), as described more fully in Attachment A-3, SERRANO's home located at 3030 Valle Vista Drive, Apartment 5, Los Angeles, CA 90065 (the "SERRANO RESIDENCE"), as described more fully in Attachment A-4, and three digital devices (collectively, the "SUBJECT DEVICES"), specifically: (1) a black Apple iPhone, model unknown, bearing IMEI number 356115090063906 ("SUBJECT DEVICE 1"), seized incident to SERRANO's arrest on October 2, 2018; (2) a grey ANS cell phone, model L50 and bearing HEX ID: 99001220509829 ("SUBJECT DEVICE 2"); and (3) a black Samsung cell phone, model SM-J727T1 and bearing IMEI: 357847094948430, as described more fully in Attachment A-5 ("SUBJECT DEVICE 3"). All the SUBJECT DEVICES are currently in the custody of the United States Postal Inspection Service in Los Angeles, California.

3. The requested search warrant seeks authorization to seize evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1704 (Possession of a Counterfeit or Unauthorized Postal Key), 18 U.S.C. § 1708 (Mail Theft and Possession of Stolen Mail), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1028(a)(7) (Unlawful Possession of a Means of Identification), 18 U.S.C. § 1029 (Access Device Fraud) and 18 U.S.C. § 371 (Conspiracy) (collectively, the "Subject Offenses"), as described more fully in Attachments B-1 and B-2. Attachments A-1 through A-6, B-1, and B-2 are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND FOR POSTAL INSPECTOR JAMES KEENAN

5. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS") and have been so employed since June 2015. I am currently assigned to the Los Angeles Division Mail Theft Team, which investigates crimes against the United States Postal Service ("USPS") and crimes related to the misuse

and attack of the mail system, including theft of United States mail, fraud, and related activity in connection with access devices (including credit and debit cards), identity theft, and unauthorized use of personal identifying information. I completed a twelve-week basic training course in Potomac, Maryland. That course included training in the investigation of identity theft by stealing from, and using, the United States mail system. Before becoming a Postal Inspector, I worked as a Customs and Border Protection Officer at the San Ysidro Port of Entry for approximately three years. I also completed a six-month basic training course at the Federal Law Enforcement Training Center. Through my discussions with other Postal Inspectors, I have learned additional information about mail theft investigations and common mail theft and identity theft practices, as well as the use of digital devices in committing related crimes.

III. SUMMARY OF PROBABLE CAUSE

6. On or about October 2, 2018, the privately-hired Chase Security Officer ("SO") Jose Bermudez entered El Dorado Lofts, a residential apartment building on 416 South Spring Street in Los Angeles, California, to begin his security duties. After entering through the glass front door, SO Bermudez saw, and confronted, SERRANO and MIRANDA as they were stealing mail from a fully-opened array of residential mailboxes and putting the mail into black trash bags. After SERRANO and MIRANDA attempted to push past SO Bermudez, SO Bermudez backed away and pulled out his Taser, ordering the men to stop. MIRANDA then fled out the

back door while SERRANO charged towards SO Bermudez, causing SO Bermudez to deploy his Taser to subdue SERRANO. During the confrontation, SO Bermudez saw SERRANO drop a set of keys, on which law enforcement later found three counterfeit arrow keys, and SUBJECT DEVICE 1. SERRANO was able to flee out the front doors by tearing the wires out of the Taser, escaped to the rooftop of another apartment building with an attached parking structure, and then injured himself by jumping off the three-story structure to the ground. SO Bermudez found SERRANO underneath a parked van. SO Bermudez deployed pepper spray to subdue SERRANO when SERRANO continued to resist, handcuffed SERRANO, and called the Los Angeles Police Department ("LAPD") for assistance. LAPD arrived, arrested SERRANO, and transported him to the hospital to receive medical assistance, where he was eventually released from law enforcement custody. The trash bags, SUBJECT DEVICE 1, and three counterfeit arrow keys left by SERRANO were recovered from the lobby of the residential apartment building. SERRANO, who initially gave officers a false name and birthdate, has an outstanding arrest warrant for violating the terms of his federal supervised release in United States v. Serrano, 16-cr-00784-SVW.

7. On or about October 17, 2018, I reviewed surveillance video from the Muir Terrance Apartments on 3961 Via Marisol in Los Angeles, California containing recordings from September 26 and September 28, 2018. I recognized SERRANO in the surveillance video stealing mail from residential mailboxes on both dates, and on September 26, 2018, recognized SERRANO with a

woman that I later identified as TORRES, SERRANO's girlfriend. Surveillance video also shows SERRANO driving the SUBJECT VEHICLE on September 26, 2018, and a black Toyota Prius with "Carmax" paper plates on September 28, 2018. On the same day, I and another Postal Inspector conducted surveillance on the SERRANO RESIDENCE, saw a stolen black Toyota Prius parked in the SERRANO RESIDENCE's parking spot. LAPD responded to the area and detained MIRANDA, who was in the front passenger's seat, and Krystal Leilani Maneja ("Maneja"), who was in the driver's seat. During the search incident to Maneja's arrest by LAPD, LAPD found a California Identification Card bearing the name of S.D.L., which Maneja admitted had been given to Maneja for Maneja's use, and that S.D.L. might not know Maneja possessed S.D.L.'s identification. SUBJECT DEVICES 2 and 3 were found in the stolen Prius along with stolen mail and checks.

IV. STATEMENT OF PROBABLE CAUSE

8. Based on my review of law enforcement reports, discussions with LAPD Officers, and my own knowledge of the investigation, I am aware of the following:

A. SERRANO and MIRANDA are Caught Stealing Mail and Flee, leaving behind Trash Bags of Stolen Mail, the SUBJECT DEVICE, and Three Counterfeit Arrow Keys

9. At approximately 6:40 a.m. on October 2, 2018, SO Bermudez[1] arrived at El Dorado Lofts to cover the security shift of a colleague who had left early due to illness. The El Dorado Lofts is a residential apartment building located on S. Spring

[1] SO Bermudez was a privately-hired security guard not acting at law enforcement's direction during the events described in this affidavit.

Street in Los Angeles. SO Bermudez noticed the SUBJECT VEHICLE parked with flashing lights blocking the bicycle lane, which SO Bermudez said was unusual because there was street parking available on the other side of the bicycle lane. SO Bermudez saw an unidentified female passenger waiting in the back passenger seat of the SUBJECT VEHICLE.

10. When he arrived, SO Bermudez saw SERRANO and MIRANDA standing in front of an array of opened residential mailboxes, pulling mail out of the boxes and stuffing it into dark plastic trash bags. SERRANO and MIRANDA attempted to leave when they saw SO Bermudez, causing SO Bermudez to ask them to remain. When SERRANO and MIRANDA attempted to push past SO Bermudez, SO Bermudez backed away, pulled out his Taser, and ordered them to stop.

11. SERRANO then charged towards SO Bermudez while MIRANDA fled through a door on the other side of the lobby. SO Bermudez deployed his Taser to subdue SERRANO, causing SERRANO to fall to the ground, and again ordered him to stop. SERRANO, however, continued to resist, and after the third Taser charge, SERRANO ripped the wires out of the Taser and fled out the front door. During this confrontation, SO Bermudez saw that SERRANO dropped a set of keys and SUBJECT DEVICE 1. SERRANO and MIRANDA also left behind the trash bags of stolen mail. SO Bermudez then pursued SERRANO while calling other security guards for assistance in locating SERRANO and recovering the trash bags and items left in the lobby, including the keys and SUBJECT DEVICE 1.

12. SERRANO fled and eventually entered the open rooftop of another residential apartment building located on S. Hill Street with an attached parking garage. SO Bermudez saw SERRANO jump off the rooftop to the ground three stories below, injuring his legs. SO Bermudez sprayed pepper spray down at SERRANO in attempt to stop SERRANO from fleeing again; however, SERRANO got up and fled again, hiding underneath a parked car in the garage.

13. SO Bermudez came down to the ground floor, where he found SERRANO hiding underneath a parked car and ordered SERRANO to come out. SERRANO again refused to comply and SO Bermudez deployed pepper spray to subdue SERRANO, pulled SERRANO out, and handcuffed him. SO Bermudez then called LAPD for assistance, and SERRANO was arrested by the LAPD Officers Armendariz and Garcia and subsequently transported to a hospital, where SERRANO was released from law enforcement custody. SERRANO has since been released from the hospital.

14. SO Bermudez returned to the El Dorado Lofts and, with the assistance of other private security officers, recovered and transferred to LAPD the trash bags, SUBJECT DEVICE 1, and a set of keys on a key ring that SERRANO dropped while attempting to flee the location. According to LAPD Officers Armendariz and Garcia, three of the keys appeared to be counterfeit postal arrow keys. Based on my training and experience, I know that counterfeit postal arrow keys are keys patterned after a special master key that opens collection boxes, residential mailboxes, and any USPS controlled mail entry/exit point that has the arrow lock installed.

15. On October 8, 2018, I tested the three counterfeit arrow keys found in the lobby of the El Dorado Lofts and confirmed that all three turned a lock issued by the United States Postal Service for the Los Angeles area; two turned the lock and did not drop it while the third was able to successfully fully open the lock.

16. SERRANO initially provided LAPD Officer Garcia with the name of "Steven Zevrano" and a birthdate of June 22, 1986, and then later provided Officer Garcia a different birthdate of September 20, 1987. LAPD was, however, unable to locate a record associated with the name "Steven Zevrano" with either date of birth. The LAPD Officers contacted USPIS, who agreed to come to the hospital to provide assistance with the follow-up mail theft investigation.[2]

B. USPIS Arrives at the Hospital to Assist with the Mail Theft Investigation

17. At approximately 12:15 p.m., Postal Inspector Chris Siouris and I arrived at the hospital and met with LAPD Officers Garcia and Armendariz, who explained the circumstances of SERRANO's arrest and showed me black garbage bags full of approximately 175 pieces of mail, 3 parcels and miscellaneous advertisement mailers. In addition, Officers Garcia and Armendariz showed me what appeared to be three counterfeit

[2] SERRANO was taken immediately to the hospital due to the severity of his leg injuries and was not Mirandized. During questioning by medical staff in the presence of law enforcement, SERRANO provided a name of "Steve Serrano" and a birthdate of September 10, 1987 and said he was 29 years of age. When I told SERRANO his age wasn't possible given the birthdate he provided, SERRANO remained silent.

postal arrow keys found on the key ring SERRANO dropped. LAPD also provided me four additional pieces of mail and two credit cards found with SERRANO when he was caught by SO Bermudez, none of which were addressed to SERRANO.

18. Postal Inspector Siouris and I agreed to take the case for federal investigation and LAPD left us at the hospital with SERRANO. LAPD Officers with the Parcel Squad and assigned to assist Postal Inspectors with federal investigations remained with SERRANO overnight in the hospital.

19. The same evening at approximately 10:47 p.m., I learned from LAPD Officer Steve Winters via text message that LAPD Officer Carmen Mederos had made contact with SERRANO's mother who confirmed SERRANO's true and correct identity of JOADLY SERRANO over the phone.

20. On the morning of October 3, 2018, I received and reviewed SERRANO's criminal history and saw that SERRANO has an outstanding federal arrest warrant for a supervised release violation. SERRANO's supervision arose from a prior mail theft conviction in United States v. Serrano, 16-cr-00784-SVW, for which SERRANO received a sentence of 366 days in prison and three years' of supervised release. I contacted the U.S. Marshals Service and the United States Probation Office that same day, who confirmed that the warrant was still outstanding. I advised the U.S. Marshals Service of SERRANO's location and condition and provided them with a contact phone number for the hospital.

21. After learning that SERRANO was likely going to require surgery, on October 3, 2018, LAPD Parcel Squad Officer Dave Holmes informed SERRANO and hospital staff that SERRANO was no longer being detained by LAPD or USPIS and would be free to leave following his surgery procedures.

C. Review of Surveillance Video from El Dorado Lofts

22. On or about October 3, 2018, Dan Joy, USPIS Senior Technical Surveillance Specialist obtained surveillance video recording the exterior of the El Dorado Lofts building, the interior of the front lobby facing the street, the elevator banks, the residential mailbox area, and the hallway leading away from the residential mailbox area to the back door of the building which I reviewed on or about October 4, 2018.

23. Based on my review of surveillance video, shortly before SO Bermudez's arrival, two males, later identified pursuant to an arrest described below as SERRANO and MIRANDA, and the female passenger used the SUBJECT VEHICLE to arrive at the El Dorado Lofts; SERRANO and MIRANDA then exited the SUBJECT VEHICLE to enter the apartment building while the female waited inside the SUBJECT VEHICLE.

24. On the surveillance video, I was also able to see SERRANO and MIRANDA enter the building, call the elevator to the ground level, and then use keys to open the residential mailboxes, take mail out, and place the mail into black trash bags. Shortly thereafter, surveillance video shows SO Bermudez arrive, enter the building, approach the area where SERRANO and MIRANDA were stealing mail, back away and pull his Taser, and

then approach. The video records the confrontation between SERRANO and SO Bermudez, MIRANDA's escape out the back door, and the female passenger's kicking and banging at the front door before driving away in the SUBJECT VEHICLE.

D. Surveillance of SERRANO and TORRES Stealing Mail at Muir Terrace

25. On or about October 11, 2018, USPIS Postal Inspector Gerardo Ramirez provided me still images of two suspected mail thieves who were video-recorded stealing mail from Muir Terrace Apartments. The theft had been reported by building management and residents, who provided the still images and later a copy of the video surveillance to Postal Inspectors. I recognized from the SERRANO as the single mail thief on September 26, 2018, and SERRANO and a female, who I later identified as TORRES after visiting the SERRANO RESIDENCE, as the two suspected mail thieves recorded on September 28, 2018.

26. On or about October 17, 2018, I obtained and reviewed the surveillance video from Muir Terrace for September 26, 2018 and September 28, 2018. The surveillance video from September 26, 2018 shows SERRANO driving the SUBJECT VEHICLE to Muir Terrace, using a key to open the residential lobby door and using a key to open residential mailboxes, from which he steals mail.

27. The surveillance video from September 28, 2018, shows SERRANO driving a black Toyota Prius with "CarMax" paper plates to Muir Terrace. SERRANO and TORRES are then shown walking up to the entrance of one of the buildings, and SERRANO hands

TORRES a bag to hold while SERRANO uses a key in the residential callbox to open the door. Once SERRANO and TORRES are inside, the video surveillance shows TORRES recalling the elevator located just to the left of the residential mailboxes and watching a nearby pedestrian entrance while SERRANO uses a key to open residential mailboxes and remove mail. Afterwards, SERRANO can be seen leaving the building with TORRES and going to another building in the same complex to remove mail from the residential mailboxes. Again, SERRANO can be seen removing delivered mail while TORRES awaits nearby, recalling the elevator and watching for tenants approaching.

28. In other clips from the September 28, 2018 surveillance video, TORRES can be seen walking through the complex with a clear bag of stolen mail that SERRANO had given to her to carry.

29. I know from my training and experience that U.S. Postal Service Arrow Keys and their counterfeits can be used to access residential buildings and the residential mailboxes inside. Furthermore, I also know from my training and experience that mail thieves will often work together and one will act as a lookout for people who may be coming by while the others take mail from the delivery boxes. In addition, mail thieves and co-conspirators will re-call elevators to the main lobby while they steal mail so they will be aware of potential persons coming from the elevator who may see their mail theft activities.

E. USPIS Visit the SERRANO RESIDENCE, Identify TORRES, and See the SUBJECT VEHICLE Parked Outside

30. On or about October 15, 2018, I pulled SERRANO's DMV record and found the SERRANO RESIDENCE listed as his place of residence. I spoke with Postal Inspector Susan Lanzl who confirmed she worked a previous mail theft investigation that involved SERRANO and had been by the SERRANO RESIDENCE to visit SERRANO on multiple occasions, and that SERRANO appears live with his child and mother. I also queried law enforcement databases and confirmed that the SERRANO RESIDENCE was the most recent address on file for SERRANO.

31. On or about October 15, 2018, I and other Postal Inspectors went to the SERRANO RESIDENCE in an attempt to return SERRANO's personal property, which was seized from his person incident to his arrest and transferred to us by LAPD Officers to return. We used our postal keys to enter the large, open parking lot of the residential apartment complex, which was separated from the sidewalk with a fence. After entering through the pedestrian gate, I saw the SUBJECT VEHICLE parked in a parking space close to the SERRANO RESIDENCE. The parking lot is an open air parking lot viewable from the street. We confirmed that license plate on the SUBJECT VEHICLE was the same as previously reported being seen on the Muir Terrance video surveillance.

32. I knocked on the door of the SERRANO RESIDENCE and a female answered the door. She identified herself as TORRES and said that she was SERRANO's girlfriend. She told us SERRANO

lived at the home but was at a doctor's appointment and that he would return later. Inspector Susan Lanzl provided TORRES with her business card and told TORRES to have SERRANO call so we could return his property to him. Based on our discussions with Postal Inspector Lanzl and surveillance of the property it appears that SERRANO, his child, and his mother live at the SERRANO RESIDENCE, and that TORRES and MIRANDA are frequently there.

33. I reviewed the DMV records for TORRES and, based on the DMV photograph and my interaction with her, confirmed that she was, in fact, TORRES and that she was the second person I saw on surveillance images assisting SERRANO during his September 28, 2018 theft of mail from Muir Terrace.

34. On or about October 16, 2018, I drove by the SERRANO RESIDENCE and saw, from the street, the SUBJECT VEHICLE still parked in the same space.

F. The Black Toyota Prius Was Determined to be Stolen, SUBJECT DEVICES 2 and 3 are Found in the Prius, and MIRANDA and Maneja are Detained and Interviewed

35. On or about October 17, 2018, I and Postal Inspector Ramirez conducted surveillance of the SERRANO RESIDENCE and saw a black Toyota Prius where the SUBJECT VEHICLE had previously been parked. Postal Inspector Ramirez re-entered the open parking lot by entering after another individual had opened the pedestrian gate to exit the parking lot. The individual held open the gate to allow Postal Inspector Ramirez to enter. Postal Inspector Ramirez saw that the Prius had paper plates and obtained the Vehicle Identification Number ("VIN") for the car,

and then returned to his USPIS car that was parked on the street. Postal Inspector Ramirez then queried law enforcement databases and determined that the Prius had been reported stolen.

36. Postal Inspector Ramirez maintained visual surveillance of the residential apartment complex from his USPIS car, while I contacted LAPD and informed them that we had located a stolen car while surveilling a mail theft suspect's residence. LAPD queried their own databases and confirmed that the Prius, with the associated VIN, had been reported stolen.

37. Postal Inspector Ramirez then saw a male and a female, get into the Prius and drive towards the exit. When the Prius approached the exit gate, however, the occupants appeared unable to open the gate and the male, who was in the front passenger's seta, got out of the car. Based on Postal Inspector Ramirez's review of still images of the October 2, 2018 mail theft at the El Dorado Lofts, he suspected that the male passenger was the second person who was stealing mail on that day with SERRANO.

38. Based on LAPD's confirmation that the Prius was a known, stolen car, LAPD responded to the area, and conducted a felony traffic stop because the Prius the occupants were driving had been reported stolen. The occupants were ordered to exit the car. The driver of the car, who was subsequently identified as Maneja, was placed under arrest, while the male passenger, who was subsequently identified as MIRANDA, was detained. Based on its status as a stolen car, the Prius was searched and impounded, and SUBJECT DEVICE 2 was found on the front driver's

seat, and SUBJECT DEVICE 3 was found in the center console area of the Prius. In addition, mail addressed to individuals not TORRES, MIRANDA, SERRANO, or Maneja was found in the Prius, along with checks also not belonging to TORRES, MIRANDA, SERRANO, or Maneja.

39. During a search for potential weapons prior to being transported, MIRANDA was found in possession of approximately 3.51 gross grams amount of suspected methamphetamine. Maneja was also later found in possession of a California Identification Card bearing the name of S.D.L., which was seized during a search of Maneja's person incident to her arrest.

40. Both MIRANDA and Maneja were transported to the LAPD Northeast Station to be interviewed regarding the stolen car. I and Postal Inspector Ramirez conducted the interview of MIRANDA. We advised MIRANDA of his Miranda rights, which he waived and consented to be interviewed. During the recorded interview, MIRANDA said he did not know the Prius was stolen and that he had come to the SERRANO RESIDENCE to use methamphetamine and borrow the Prius. MIRANDA admitted to being with SERRANO the night of the El Dorado Lofts mail theft, but denied stealing mail, and denied knowing the identity of the female who had been seen in the Prius parked outside and had banged on the glass front door when SO Bermudez caught SERRANO and MIRANDA stealing mail. MIRANDA, however, became quiet when presented with surveillance images of MIRANDA and SERRANO stealing mail on October 2, 2018. I subsequently ended the interview and MIRANDA was taken into federal custody.

41. During the interview of Maneja, she admitted that SUBJECT DEVICE 2 was her cell phone, and denied knowing about the mail or checks found in the Prius. However, when asked if her fingerprints would be found on the documents or the area where they were found, she admitted that she may have rummaged through the area where they were found in the Prius. Furthermore, she admitted to knowingly possessing the counterfeit identification card bearing the name "Sandra Dolores Lopez," and that it had been given to Maneja by a friend.

V. TRAINING AND EXPERIENCE REGARDING MAIL AND IDENTITY THEFT

42. Based on my training and experience and information obtained from other law enforcement officers who investigate mail and identity theft, I know the following:

a. People who steal mail are often involved in fraud and identity theft crimes. These individuals usually steal mail looking for checks, access devices, other personal identifying information (such as names, Social Security numbers, and dates of birth), and identification documents that they can use to fraudulently obtain money and items of value. Mail thieves often retain these items of value from stolen mail in order to make fraudulent purchases or sell the items to others in exchange for cash or drugs.

b. Mail thieves also commonly store their stolen mail, access devices, false identification materials, stolen keys, and other materials used to in the commission of mail theft and identity theft on or in areas they control or have repeat access to, such as their persons, their residences, cars,

or cars driven by them or other accomplices, witting or unwitting, to locations to steal mail, such as the SERRANO RESIDENCE and the SUBJECT VEHICLE.

c. It is common practice for individuals involved in mail theft, identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once in their residences and the cars used to steal mail. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

d. Often times mail and identity thieves take pictures of items retrieved from stolen mail or mail matter with their cellphones.

e. It is also common for mail and identity thieves to keep "profiles" of victims on digital devices. Such

"profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

f. It is common for mail thieves, identity thieves, and individuals engaged in bank fraud, access device fraud, and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. Such people often store their devices on their person, inside their residences, and in their cars. Software relevant to such schemes can often be found on digital devices, such as computers.

g. Based on my training and experience, I know that individuals who participate in mail theft, identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos.

h. Individuals engaged in mail and identity theft often use multiple digital devices that are stored on their person or in areas they control or have access to, such as the SERRANO RESIDENCE and the SUBJECT VEHICLE.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

43. As used herein, the term "digital device" includes the SUBJECT DEVICES.

44. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital data in a single day or even over several weeks for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result,

a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The SUBJECT DEVICES contain multiple gigabytes of storage space. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[3] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or

[3] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has

been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the

absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

45. As discussed herein, based on my training and experience I believe that digital devices may be recovered from the search of SERRANO and TORRES's persons, the SUBJECT VEHICLE, and the SERRANO RESIDENCE that are enabled with biometric unlock functionality.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-

recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring

2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

46. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

47. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric

features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

48. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device.

49. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to: (1) compel the use of SERRANO or TORRES's thumb- and/or fingerprints on the device; and (2) hold the device in front of SERRANO or TORRES's face with their eyes open to activate the facial-, iris-, and/or retina-recognition feature for digital devices found on TORRES's or SERRANO's person, the SERRANO RESIDENCE, or in the SUBJECT VEHICLE. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

50. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

51. For all of the reasons described above, there is probable cause to believe that SERRANO, MIRANDA, and TORRES have committed a violation of Title 18, United States Code, Sections 1708 and 2 (Mail Theft and Aiding and Abetting Mail Theft). There is also probable cause that the items to be seized described in Attachment B-1 will be found in a search of the person of SERRANO, the person of TORRES, the SUBJECT VEHICLE, and the SERRANO RESIDENCE, as described in Attachments A-1, A-2, A-3, and A-4, respectively, and that that the items to be seized described in Attachment B-2 will be found in the SUBJECT DEVICES, as described in Attachment A-5.

/s/
James M. Keenan, Special Agent
United States Postal
Inspection Service

Subscribed to and sworn before me
this 18th day of October, 2018.

Suzanne H. Segal
THE HONORABLE SUZANNE H. SEGAL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

PERSON TO BE SEARCHED

The person of JOADLY SERRANO ("SERRANO"), date of birth of September 10, 1990, with California Driver's License Number D7488052. SERRANO's California Department of Motor Vehicle records lists him as standing five foot, ten inches with brown hair and hazel eyes.

The search of SERRANO shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within SERRANO's immediate vicinity and control at the location where the search warrant is executed.

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person of YESENIA TORRES ("TORRES"), date of birth of January 13, 1992, with California Driver's License Number D6805011. TORRES's California Department of Motor Vehicle records lists her as standing 5 feet and 4 inches tall with brown hair and brown eyes.

The search of TORRES shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within TORRES's immediate vicinity and control at the location where the search warrant is executed.

ATTACHMENT A-3

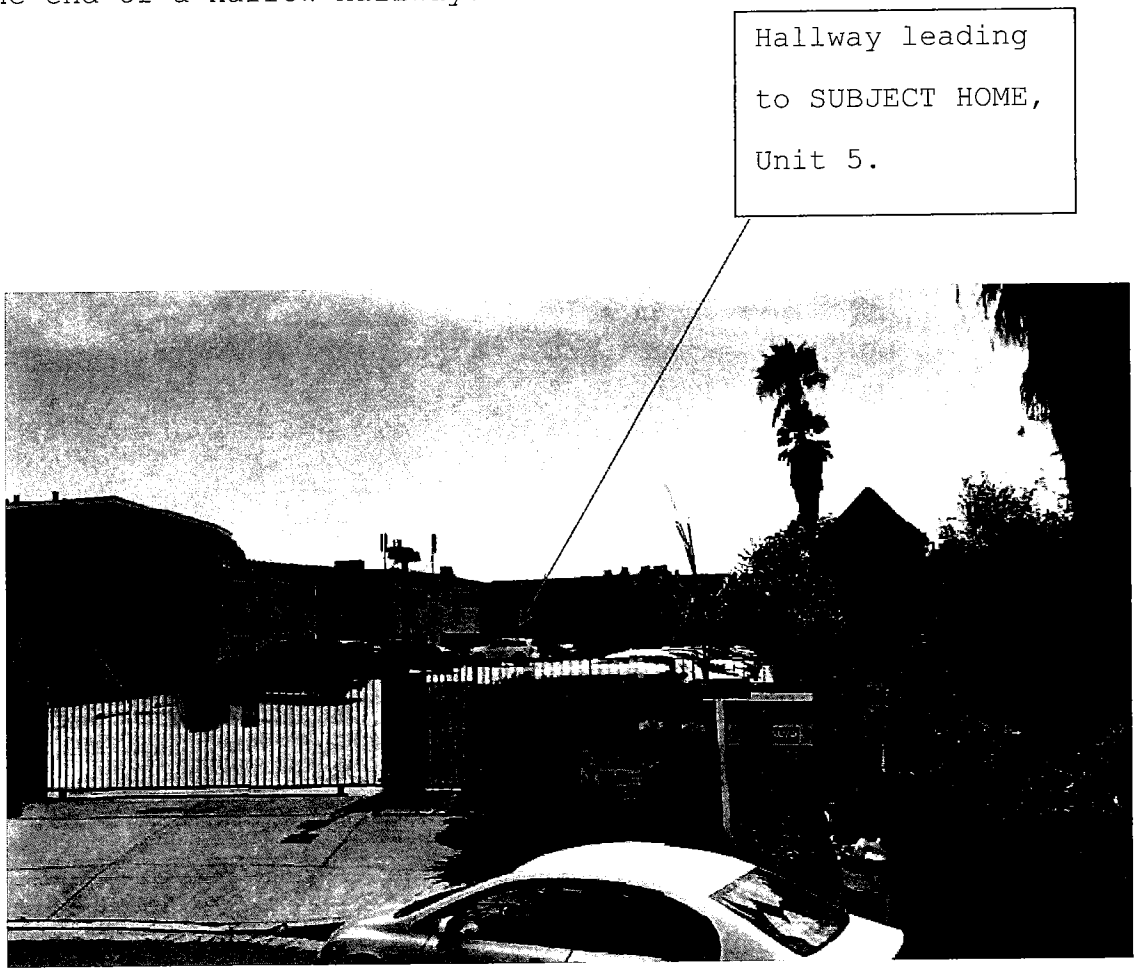
PROPERTY TO BE SEARCHED

A red 2017 Toyota with California license plate tag 7ZOT239 and Vehicle Identification Number 5YFBURHE4HP736104 (the "SUBJECT VEHICLE") wherever it may be located within the Central District of California.

ATTACHMENT A-4

PROPERTY TO BE SEARCHED

A residence located at 3030 Valle Vista Drive, Unit 5, Los Angeles, California 90065 (the "SERRANO RESIDENCE"). The SERRANO RESIDENCE is located on the north end of the residential building complex as you face the parking lot entrance. The building the SERRANO RESIDENCE is located in is painted tan in color and the number "5" is displayed on the center of the door of the SERRANO RESIDENCE, which is located on the left side at the end of a narrow hallway.



ATTACHMENT A-5

PROPERTY TO BE SEARCHED

1. A black Apple iPhone of an unknown model bearing IMEI number 356115090063906 ("SUBJECT DEVICE 1"), which was seized on or about October 2, 2018, incident to SERRANO's arrest;

2. A grey ANSA cell phone, model L50 and bearing HEX ID: 99001220509829 ("SUBJECT DEVICE 2"), seized incident to Krystal Leilani Maneja ("Maneja's") arrest on or about October 17, 2018 from the driver's seat of a black Toyota Prius; and

3. A black Samsung cell phone, SM-J727T1 and bearing IMEI: 357847094948430, recovered from the center console of a black Toyota Prius that was impounded on or about October 17, 2018 ("SUBJECT DEVICE 3", together with SUBJECT DEVICE 1 and SUBJECT DEVICE 2, the "SUBJECT DEVICES").

All the SUBJECT DEVICES are currently in the custody of the United States Postal Inspection Service in Los Angeles, California.

ATTACHMENT B-1

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1704 (Possession of a Counterfeit or Unauthorized Postal Key), 18 U.S.C. § 1708 (Mail Theft and Possession of Stolen Mail), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1028(a)(7) (Unlawful Possession of a Means of Identification), 18 U.S.C. § 1029 (Access Device Fraud) and 18 U.S.C. § 371 (Conspiracy) (collectively, the "Subject Offenses"), namely:

a. Data, records, documents, or information (including electronic mail and messages) pertaining to obtaining, possessing, using, or transferring personal and/or financial transaction identification information for persons other than SERRANO, MIRANDA, TORRES, or Maneja, such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, email addresses, IP addresses, as well as PIN numbers and passwords for financial institutions or internet service providers;

b. Records, documents, programs, applications, or materials pertaining any bank accounts, credit card accounts, or other financial accounts, including applications for, or use of, credit or debit cards, bank accounts, or merchant processor accounts;

c. Data, records, documents (including e-mails), or information reflecting or referencing purchases of merchandise, securities, electronic currency, and other valuable things;

d. Records, documents, programs, applications, or materials relating to United States mail or mail matter;

e. U.S. currency in excess of $1,000, including the first $1,000 if more than $1,000 is recovered, bearer instruments worth over $1,000 (including cashier's checks and traveler's checks), and precious stones worth more than $1,000;

f. Any altered, counterfeit, or fraudulent identifications, checks, access devices, monetary instruments, or other official documents;

g. Any documents or records, including receipts, invoices, bank statements, and credit card statements, evidencing the purchase of any products or services using altered, counterfeit, or fraudulent or unauthorized checks, access devices, or other monetary instruments;

h. Any products, goods, or merchandise purchased with fraudulent or unauthorized checks, access devices, or other monetary instruments;

i. Any identifications, checks, access devices, monetary instruments, or other official documents that are not addressed to, or in the name of, SERRANO, MIRANDA, TORRES, or Maneja;

j. Any tools or equipment, such as computers, software, printers, scanners, embossing machines, credit card readers or encoders, washing chemicals, or imprinting tools,

used or intended to be used to alter, counterfeit, or create fraudulent checks, access devices, or other monetary instruments;

k. Records of off-site storage locations, including safe-deposit box keys, records, receipts, or rental agreements for storage facilities;

l. Indicia of occupancy, residency or ownership of the SUBJECT PREMISES and things described in the warrant, including forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease of rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

m. Contents of any calendar or date book stored on any of the digital devices;

n. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

o. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

p. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers

accessed through any push-to-talk functions, as well as all received or missed incoming calls;

q. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

r. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

s. Audio recordings, pictures, video recordings, or still captured images of United States mail or mail matter, whether opened or unopened, or relating to the possession or distribution of drugs or the collection or transfer of the proceeds of the above-described offenses; and

t. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were

created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool

Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period,

obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, law enforcement personnel are authorized to: (1) depress SERRANO or TORRES's thumb- and/or fingerprints onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific fingers and/or thumbs shall be depressed; and (2) hold the device in front of SERRANO or TORRES's face with their eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT B-2

III. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1704 (Possession of a Counterfeit or Unauthorized Postal Key), 18 U.S.C. § 1708 (Mail Theft and Possession of Stolen Mail), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1028(a)(7) (Unlawful Possession of a Means of Identification), 18 U.S.C. § 1029 (Access Device Fraud) and 18 U.S.C. § 371 (Conspiracy) (collectively, the "Subject Offenses"), namely:

a. Data, records, documents, or information (including electronic mail and messages) pertaining to obtaining, possessing, using, or transferring personal and/or financial transaction identification information for persons other than SERRANO, MIRANDA, TORRES, or Maneja, such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, email addresses, IP addresses, as well as PIN numbers and passwords for financial institutions or internet service providers;

b. Records, documents, programs, applications, or materials pertaining to applications for, or use of, credit or debit cards, bank accounts, or merchant processor accounts;

c. Data, records, documents (including e-mails), or information reflecting or referencing purchases of merchandise, securities, electronic currency, and other valuable things;

d. Software, devices, or tools used to obtain, create, or use counterfeit or unauthorized checks, coupons, or access devices such as credit, debit, bank, and gift cards;

e. Any documents or records relating to any bank accounts, credit card accounts, or other financial accounts;

f. Records, documents, programs, applications, or materials relating to United States mail or mail matter;

g. Contents of any calendar or date book stored on any of the digital devices;

h. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

i. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

j. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

k. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

l. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

m. Audio recordings, pictures, video recordings, or still captured images of United States mail or mail matter, whether opened or unopened, or relating to the possession or distribution of drugs or the collection or transfer of the proceeds of the above-described offenses; and

n. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

o. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

IV. SEARCH PROCEDURE FOR DIGITAL DEVICES

3. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICES as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital devices beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or

encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. If the search team, while searching a SUBJECT DEVICE, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that SUBJECT DEVICE pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that a SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.